Quantum states representing perfectly secure bits are always distillable

Paweł Horodecki* and Remigiusz Augusiak†
Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gdańsk, Poland
(Dated: February 1, 2008)

It is proven that recently introduced states with perfectly secure bits of cryptographic key (private states representing secure bit) [K. Horodecki *et al.*, Phys. Rev. Lett. **94**, 160502 (2005)] as well as its multipartite and higher dimension generalizations always represent distillable entanglement. The corresponding lower bounds on distillable entanglement are provided. We also present a simple alternative proof that for any bipartite quantum state entanglement cost is an upper bound on distillable cryptographic key in bipartite scenario.

PACS numbers:
Keywords:

I. INTRODUCTION

For a long time quantum cryptography with entanglement discovered by Ekert [1] has been developed based on pure quantum entanglement as a central resource. More precisely the schemes (see Ref. [2]) existing in this domain were equivalent to entanglement distillation [3]. Recently it has been shown that entanglement which is not distillable (bound entanglement) can provide a quantum cryptographic key [4]. This leads to a general scheme of key distillation from quantum states [4, 5] with a private state representing a secure bit (alternatively: a private bit state or private bit) as an important notion. The latter is a quantum state shared by Alice and Bob that contains at least one bit of perfectly secure cryptographic key. Quite nonintuitively, private bits can be approximated arbitrary well by some bound entangled states in some special sense: there exist a sequence of private bits with dimension of their "shield" part going to infinity and another sequence of bound entangled states such that trace distance between elements of the two sequences goes to zero [4, 5]. Here we show that despite of that fact any single private bit is distillable. Using local filtering [6] in a way exploited in Ref. [7] we provide a lower bound on the corresponding distillable entanglement of d–dimensional private state (d-dimensional generalization of p-bit). Note that the special (bipartite) case of our result has already found an important application in a proof of unconditional cryptographic security with small distillable entanglement [8]. Finally we give a simple alternative proof that for any bipartite state entanglement cost E_C (see Refs. [9, 10]) is an upper bound on amount of a distillable cryptographic key K_D (usually called distillable key). Originally this was proven [4, 5] from the fact that regularized entropy of entanglement E_R^∞ is an upper bound for K_D. We provide a simpler version that does not need to refer to E_R^∞.

*Electronic address: pawel@mif.pg.gda.pl
†Electronic address: remik@mif.pg.gda.pl

II. LOWER BOUNDS ON DISTILLABILITY

A. Distillation of entanglement from private bits

For purely pedagogical reasons at the very beginning we shall derive the lower bound on distillable entanglement of private bits. This is the starting point for more general classes of secure states as d–dimensional private states and their multipartite counterparts.

Let us recall the definition of private bit [4, 5]. This is the bipartite state with internal structure of both Alice and Bob systems. It is defined on four-partite Hilbert space $\mathcal{H}_{ABA'B'} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ with subsystems denoted by A and A' (B and B') belonging to Alice (Bob). The first pair of subsystems shared by Alice and Bob is of qubit structure, i.e., $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B \sim \mathbb{C}^2 \otimes \mathbb{C}^2$, while the second one has in general the form $\mathcal{H}_{A'B'} = \mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \sim \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_{B'}}$. The explicit form of private bit is

$$\gamma^{(2)}_{ABA'B'} \equiv \gamma^{(2)} = \frac{1}{2} \sum_{i,j=0}^{1} |ii\rangle\langle jj| \otimes U_i \rho_{A'B'} U_j^\dagger, \quad (2.1)$$

where $\{|ij\rangle\}$ is the standard two-qubit product basis in $\mathcal{H}_{AB}$, $\rho_{A'B'}$ denotes some state acting on $\mathcal{H}_{A'B'}$ and U_i ($i = 0, 1$) are some unitary operations. The structure of private bit can be divided into two parts [5]. The first one (AB) called *key part* is the one from which Alice and Bob can get a bit of secure key after local measurements in the standard bases. The second part ($A'B'$) is called *shield part* (in the case of approximate private bits this part in a sense "defends" the key in system AB from an eavesdropper in the asymptotic regime [5]). We must stress that the private bit contains the *perfectly* secure bit of key while it can be approximated by bound entangled states in the sense that there exist a sequence of private bits $\gamma_k^{(2)}$ with the dimension of their shield parts $\mathcal{H}^{(k)}_{A'B'}$ going to infinity and another sequence of bound entangled states ϱ_k such that for any ϵ there exist k such that $||\gamma_k^{(2)} - \varrho_k|| \leq \epsilon$. The latter has been proven to imply that a bound entangled state can contain *secure bit up to arbitrary precision* measured by ϵ in the sense

that the eavesdropper information about the shared bit is bounded by some continuous function of ϵ that vanishes for $\epsilon = 0$ (see Ref. [5]). In general one has a perfectly secure bit (no Eve's knowledge about the bit) for $\epsilon = 0$, i.e., when the observers share just a private bit. It turns out that this exact case can never happen when the observers are given bound entanglement since, according to main result of the present paper, a private bit is always distillable.

Having reviewed the structure of $\gamma^{(2)}$, we can start a description of distillation protocol. We define the following parameter

$$\eta = \max \left| \langle e_1| \otimes \langle f_1|U_0\rho_{A'B'}U_1^\dagger|e_2\rangle \otimes |f_2\rangle \right|, \qquad (2.2)$$

where the maximum is taken over all normalized product vectors $|e_1\rangle \otimes |f_1\rangle$ and $|e_2\rangle \otimes |f_2\rangle$ belonging to $\mathcal{H}_{A'B'}$.

One immediately infers that

$$\eta \geq \max_{\substack{m,n=0,\ldots,d_{A'}-1 \\ \mu,\nu=0,\ldots,d_{B'}-1}} \left| \left[U_0\rho_{A'B'}U_1^\dagger \right]_{m\mu,n\nu} \right| > 0,$$

where strict positivity follows from the fact that the matrix representation $[U_0\rho_{A'B'}U_1^\dagger]_{m\mu,n\nu}$ of the nonzero operator $U_0\rho_{A'B'}U_1^\dagger$ in standard basis $\{|ij\rangle\}$ must have at least one nonzero element. Let $|\tilde{e}_1\rangle \otimes |\tilde{f}_1\rangle$ and $|\tilde{e}_2\rangle \otimes |\tilde{f}_2\rangle$ be product vectors from $\mathcal{H}_{A'B'}$ for which the maximum in (2.2) is achieved. Then we define numbers

$$a_s = \langle \tilde{e}_s| \otimes \langle \tilde{f}_s|U_{s-1}\rho_{A'B'}U_{s-1}^\dagger|\tilde{e}_s\rangle \otimes |\tilde{f}_s\rangle \qquad (s = 1, 2).$$

These numbers are always positive and the square root of their product is bounded from below by η (see Ref. [11]). Now we are in a position to show the distillability of $\gamma^{(2)}$. Let us assume that $a_2 \geq a_1 > 0$. Then we define local operators:

$$V_{AA'} = |0\rangle\langle 0| \otimes \langle \tilde{e}_1| + \sqrt{\frac{a_1}{a_2}}\, \mathrm{e}^{\mathrm{i}\Theta} |1\rangle\langle 1| \otimes \langle \tilde{e}_2|,$$

with

$$\Theta = \arg \left[\langle \tilde{e}_1| \otimes \langle \tilde{f}_1|U_0\rho_{A'B'}U_1^\dagger|\tilde{e}_2\rangle \otimes |\tilde{f}_2\rangle \right],$$

and

$$P_{BB'} = |0\rangle\langle 0| \otimes \langle \tilde{f}_1| + |1\rangle\langle 1| \otimes \langle \tilde{f}_2|.$$

The above operators can be used in LOCC operation of two-way type. The operation (called two-way local filtering) produces with probability $a_1 > 0$ the state:

$$\begin{aligned} \varrho \;&\equiv\; \frac{V_{AA'} \otimes P_{BB'}\gamma^{(2)}_{ABA'B'}V_{AA'}^\dagger \otimes P_{BB'}^\dagger}{\mathrm{Tr}\left[V_{AA'} \otimes P_{BB'}\gamma^{(2)}_{ABA'B'}V_{AA'}^\dagger \otimes P_{BB'}^\dagger \right]} \\ &=\; p|\Psi_+\rangle\langle\Psi_+| + (1-p)|\Psi_-\rangle\langle\Psi_-|, \end{aligned} \qquad (2.3)$$

with $p = (1/2)(1 + \eta/\sqrt{a_1a_2})$ and two Bell states $|\Psi_\pm\rangle = (1/\sqrt{2})(|00\rangle \pm |11\rangle)$. Distillable entanglement of two-element mixture of Bell states is known to be [12, 13] $E_D(\varrho) = 1 - H(p)$, where $H(p) = -p\log p - (1-p)\log(1-p)$ and can be achieved in the so–called hashing protocol [13]. If $a_1 \geq a_2$ one applies the same procedure with only one modification, i.e., putting the local filter $W_{AA'} = \sqrt{a_2/a_1}\mathrm{e}^{-i\Theta}V_{AA'}$ in place of $V_{AA'}$. The resulting state is equal to the same mixture of Bell states (2.3) as in the previous case, but the probability of its production is now a_2. Combining these two observations we have the lower bound on distillable entanglement of $\gamma^{(2)}$:

$$E_D\left(\gamma^{(2)}\right) \geq a_{\max}\left[1 - H\left(\frac{1}{2} + \frac{\eta}{2\sqrt{a_1a_2}} \right) \right], \qquad (2.4)$$

where the factor $a_{\max} = \max[a_1, a_2]$ is maximum of two probabilities of production of the considered two-qubit Bell states mixture. It should be emphasized that $\eta > 0$ and therefore the Shannon entropy in (2.4) is less than one, which results in strict positivity of right–hand side of (2.4). Thus a bipartite private bit is always a distillable state.

B. Distillability of multipartite p-dits

Here we shall provide a generalization of the result to any multipartite version of a bipartite d–dimensional private state (hereafter denotes by $\gamma^{(d)}_{ABA'B'}$ or shortly by $\gamma^{(d)}$) [4, 5]. Multipartite d–dimensional private states play a natural role in the generalized scheme of distillation of a secure key in a multipartite scenario [14]. As mentioned, the special case of the present result, i.e., the $\gamma^{(d)}$ one has already been applied in an unconditional security proof with a small distillable entanglement [8].

A multipartite d–dimensional private state is a natural generalization of the private bit (2.1) both in the "size" of the key part (increased for any local observer from dimension 2 to d; this leads to $\log d$ of secure bits of key [4]) and in the number of observers involved [14]: from two observers Alice (AA') and Bob (BB') to N ones $\{(A_1A_1'), (A_2A_2'), \ldots, (A_NA_N')\}$. It obviously reproduces the bipartite d–dimensional private state [4] in case of two observers. The form of multipartite (N-partite) d–dimensional private state is

$$\Gamma^{(d)}_{\mathsf{AA'}} = \frac{1}{d}\sum_{i,j=0}^{d-1} |i\ldots i\rangle\langle j\ldots j| \otimes U_i\varrho_{\mathsf{A'}}U_j^\dagger,$$

The above state is defined on a Hilbert space $\mathcal{H}_{\mathsf{AA'}} = \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{A'}} \equiv (\mathcal{H}_{A_1} \otimes \ldots \otimes \mathcal{H}_{A_N}) \otimes (\mathcal{H}_{A_1'} \otimes \ldots \otimes \mathcal{H}_{A_N'})$. Here the system $\mathsf{A} = A_1\ldots A_N$ is of $d^{\otimes N}$ type (one has N systems of d-level type instead of two systems of qubit type) with the standard basis $\{|i_1\ldots i_N\rangle\}$. The density matrix $\varrho_{A_1'\ldots A_N'}$ acting on a Hilbert space $\mathcal{H}_{\mathsf{A'}}$ is responsible for the shield part of $\Gamma^{(d)}_{\mathsf{AA'}}$ and, as previously, U_i ($i = 0, \ldots, d-1$) are certain unitary evolutions.

The distillation scheme may be found using similar techniques as for private bits. Therefore for fixed i and

j $(i<j,\ i,j=0,\ldots,d-1)$ let us define

$$\eta^{(ij)}=\max\Big|\langle f_1|\otimes\ldots\otimes\langle f_N|U_i\varrho_{\mathsf{A}'}U_j^\dagger|g_1\rangle\otimes\ldots\otimes|g_N\rangle\Big|, \tag{2.5}$$

where maximum is taken over all product vectors from $\mathcal{H}_{\mathsf{A}'}$. Similarly as in the private bit case we also define

$$a_1^{(ij)}=\langle\tilde{f}_1^{(ij)}|\otimes\ldots\otimes\langle\tilde{f}_N^{(ij)}|U_i\varrho_{\mathsf{A}'}U_i^\dagger|\tilde{f}_1^{(ij)}\rangle\otimes\ldots\otimes|\tilde{f}_N^{(ij)}\rangle,$$

and

$$a_2^{(ij)}=\langle\tilde{g}_1^{(ij)}|\otimes\ldots\otimes\langle\tilde{g}_N^{(ij)}|U_j\varrho_{\mathsf{A}'}U_j^\dagger|\tilde{g}_1^{(ij)}\rangle\otimes\ldots\otimes|\tilde{g}_N^{(ij)}\rangle$$

where $|\tilde{f}_1^{(ij)}\rangle\otimes\ldots\otimes|\tilde{f}_N^{(ij)}\rangle$ and $|\tilde{g}_1^{(ij)}\rangle\otimes\ldots\otimes|\tilde{g}_N^{(ij)}\rangle$ are vectors realizing a maximum in Eq. (2.5). In a full analogy to the case of a private bit, one checks that (cf. [11]) $0<\eta^{(ij)}\leq\sqrt{a_1^{(ij)}a_2^{(ij)}}$. Again, if for a given pair of indices $\{i,j\}$ $(i<j)$ one has $a_2^{(ij)}\geq a_1^{(ij)}>0$, we define

$$V^{(ij)}_{A_1A_1'}=|i\rangle\langle i|\otimes\langle\tilde{f}_1^{(ij)}|+\sqrt{a_1^{(ij)}/a_2^{(ij)}}\,\mathrm{e}^{\mathrm{i}\Theta_{ij}}|j\rangle\langle j|\otimes\langle\tilde{g}_1^{(ij)}|,$$

where

$$\Theta_{ij}=\arg\Big[\langle\tilde{f}_1^{(ij)}|\ldots\langle\tilde{f}_N^{(ij)}|U_i\varrho_{\mathsf{A}'}U_j^\dagger|\tilde{g}_1^{(ij)}\rangle\ldots|\tilde{g}_N^{(ij)}\rangle\Big],$$

while in the case $a_1^{(ij)}\geq a_2^{(ij)}>0$ we take $W^{(ij)}_{A_1A_1'}=\sqrt{a_2^{(ij)}/a_1^{(ij)}}\,\mathrm{e}^{-i\Theta_{ij}}V^{(ij)}_{A_1A_1'}$. Finally we introduce

$$P^{(ij)}_{A_kA_k'}=|i\rangle\langle i|\otimes\langle\tilde{f}_k^{(ij)}|+|j\rangle\langle j|\otimes\langle\tilde{g}_k^{(ij)}|\quad(k=2,\ldots,N).$$

In both cases for given i and j $(i<j)$, we shall obtain the same state but with different probabilities, $a_1^{(ij)}$ in the first case and $a_2^{(ij)}$ in the second one. The corresponding LOCC filtering performed by all N parties (the first party uses $V^{(ij)}_{A_1A_1'}$ or $W^{(ij)}_{A_1A_1'}$ while all the others apply $P^{(ij)}_{A_kA_k'}$ in full analogy to the formula (2.3)) finally gives the state

$$\varrho_N^{(ij)}=p^{(ij)}|\tilde{\Psi}_+^{(ij)}\rangle\langle\tilde{\Psi}_+^{(ij)}|+(1-p^{(ij)})|\tilde{\Psi}_-^{(ij)}\rangle\langle\tilde{\Psi}_-^{(ij)}|, \tag{2.6}$$

which is the mixture of two projectors onto GHZ states $|\tilde{\Psi}_\pm^{(ij)}\rangle=(1/\sqrt{2})(|i\ldots i\rangle\pm|j\ldots j\rangle)$ with $p^{(ij)}=(1/2)\big[1+\eta^{(ij)}/(a_{ij}^{(1)}a_{ij}^{(2)})^{1/2}\big]$. Using the GHZ distillation hashing protocol [15] (which is a generalization of that from [13]) and taking into account the fact that here one has only the so–called phase error (corresponding to the sign $\pm$ in the above formula) we get lower bound for the distillation rate of the GHZ states from $\Gamma^{(d)}_{\mathsf{AA}'}$ in the scenario with chosen filtering corresponding to a fixed pair of indices $\{i,j\}$ as below

$$E_D^{(ij)}\big(\Gamma^{(d)}_{\mathsf{AA}'}\big)\geq a_{\max}^{(ij)}\left[1-H\left(\frac{1}{2}+\frac{\eta^{(ij)}}{\sqrt{a_1^{(ij)}a_2^{(ij)}}}\right)\right]\equiv\tilde{E}_D^{(ij)}$$

with $a_{\max}^{(ij)}$ being the bigger from two numbers $a_1^{(ij)}$ and $a_2^{(ij)}$. Again, since all $\eta^{(ij)}$ are positive the above lower bounds are strictly positive too, which results in distillability of GHZ from *any* multipartite d–dimensional private state. Since we can optimize over choices of $\{i,j\}$ we get the final lower bound on distillable entanglement of $\Gamma^{(d)}_{\mathsf{AA}'}$

$$E_D\big(\Gamma^{(d)}_{\mathsf{AA}'}\big)\geq\max_{\substack{i,j=0,\ldots,d-1\\(i<j)}}\tilde{E}_D^{(ij)},$$

which again is strictly positive since, as previously proven, all quantities $\tilde{E}_D^{(ij)}$ are strictly positive.

The above protocols are working for any dimensions d. However, for $d\geq 4$, further generalization of efficiency of distillation protocol can be introduced. This is because all local projections are here two-dimensional. It is easy to generalize the above scheme in such a way that instead of single filtering of that type we perform POVM involving k filterings $(2k\geq d)$ which are locally orthogonal in the sense that their supports (subspaces on which they give nonzero results) are *disjoint*. Each of the results corresponding to kth result of POVM would produce some mixture of type (2.6). Such a scheme would be, to some extent, analogous to distillation of entanglement from mixtures of locally orthogonal states [16] which was independently analyzed also in [17].

III. BOUND ON DISTILLABLE KEY: AN ALTERNATIVE PROOF

In this section we come back again to the bipartite scenario. We bound from above the amount of a distillable cryptographic key $K_D(\varrho)$ of any given state ϱ by its entanglement cost $E_C(\varrho)$. This fact has already been proven in Ref. [5] through the regularized relative entropy of entanglement. The present proof has a more direct character and is based on the well–known facts from the theory of entanglement measures [10]. It also exploits the special structure of the eigenvectors of the bipartite d–dimensional private states.

The crucial role is played here by the asymptotic continuity of entanglement of formation [13] proved by Nielsen [18] and the fact that the entanglement cost which has a rather complicated definition (see [10]) may be related to entanglement of formation in a simple way by [9]

$$E_C(\rho)=\lim_{m\to\infty}\frac{E_F(\rho^{\otimes m})}{m} \tag{3.7}$$

for any given state ρ. Moreover, for these two measures we have $E(\Lambda(\rho))\leq E(\rho)$ with Λ being some LOCC protocol [19].

At the very beginning we show that entanglement of formation of $\gamma^{(d)}_{ABA'B'}$ [4] corresponding here just to bipartite version of $\Gamma^{(d)}_{\mathsf{AA}'}$ with d being the dimension of $\mathcal{H}_A$ (equivalently $\mathcal{H}_B$), may be bounded from below by $\log d$.

This can be obtained simply by utilizing the definition of entanglement of formation which for a given density matrix ρ acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ reads

$$E_F(\rho) = \min_{\{p_i, |\Psi_i\rangle\}} \sum_i p_i S_{\rm vN}\left(\mathrm{Tr}_B |\Psi_i\rangle\langle\Psi_i|\right),$$

where the minimum is taken over all ensembles $\{p_i, |\Psi_i\rangle\}$ generating the state ρ and $S_{\rm vN}$ stands for the von Neumann entropy [20].

Consider now the state $\gamma^{(d)}_{ABA'B'}$. One may easily see that all its eigenvectors corresponding to nonzero eigenvalues are

$$\begin{aligned} |\psi_k\rangle &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle \otimes U_j |\varphi_k^{(A'B')}\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle \otimes |\varphi_{j,k}^{(A'B')}\rangle. \end{aligned}$$

An arbitrary vector $|\Psi_i\rangle$ from any ensemble $\{p_i, |\Psi_i\rangle\}$ realizing the considered state must be a linear combination of the above eigenvectors $|\psi_k\rangle$. This is a consequence of the fact, proved in Ref. [21], that the vector $|\Psi_i\rangle$ belongs to $\mathrm{Ran}\gamma^{(d)}$, which in turn is a subspace spanned by eigenvectors $|\psi_k\rangle$. Therefore it is not difficult to see that $|\Psi_i\rangle = (1/\sqrt{d}) \sum_{j=0}^{d-1} |jj\rangle \otimes |\tilde{\varphi}_{j,k}^{(A'B')}\rangle$ must hold for some vectors $|\tilde{\varphi}_{j,k}^{(A'B')}\rangle$. Entanglement of formation of the vector $|\Psi_i\rangle$ can be easily estimated

$$\begin{aligned} E_F(|\Psi_i\rangle) &= S_{\rm vN}\big(\mathrm{Tr}_{BB'} |\Psi_i\rangle\langle\Psi_i|\big) = \\ &= \frac{1}{d} \sum_j S_{\rm vN}\big(\Xi_{j,k}^{(A')}\big) + \log d \\ &\geq \log d, \end{aligned}$$

where $\Xi_{j,k}^{(A')} = \mathrm{Tr}_{B'} |\tilde{\varphi}_{j,k}^{(A'B')}\rangle\langle\tilde{\varphi}_{j,k}^{(A'B')}|$. Since this holds for any vector from any ensemble of $\gamma^{(d)}$, we have, by the very definition of E_F, the following

Property 1. For any p-dit state $\gamma^{(d)}$ one has

$$E_F\big(\gamma^{(d)}\big) \geq \log d. \tag{3.8}$$

Note by the way that, by inspection, one can see that tensor product $(\gamma^{(d)})^{\otimes m}$ has a structure of $\gamma^{(d^m)}$ type. Hence, a straightforward application of (3.7) to $\gamma^{(d)}$ in place of ϱ together with the above inequality leads to a stronger result, namely one has

Property 1a. For any p-dit state $\gamma^{(d)}$ one has:

$$E_C\big(\gamma^{(d)}\big) \geq \log d.$$

Now we are in position to relate K_D and E_C. Suppose that Alice and Bob share n copies of a given bipartite state ϱ with $K_D(\varrho) > 0$ (for states with $K_D(\varrho) = 0$ the inequality is trivially true). Consider the optimal protocol distilling $K_D(\varrho)$ secret bits from ϱ which is a sequence of LOCC protocols Λ_n ($n \in \mathbb{N}$) such that $\Lambda_n\big(\varrho^{\otimes n}\big) = \sigma^{(n)}$ and $||\sigma^{(n)} - \gamma^{(d_n)}||_{\rm Tr} \leq \epsilon_n$ for sequence of private states $\gamma^{(d_n)}$ with the key part AB defined on the Hilbert space $\mathbb{C}^{d_n} \otimes \mathbb{C}^{d_n}$. The sequence $\{\epsilon_n\}$ is supposed to converge to zero with increasing n. Since the protocol is optimal we have by definition [5] $K_D(\varrho) = \lim_n(\log d_n/n)$.

On the other hand the asymptotic continuity of E_F together with its monotonicity under LOCC protocol implies the following inequalities:

$$\begin{aligned} \frac{1}{n} E_F\big(\gamma^{(d_n)}\big) &\leq \frac{1}{n} E_F\big(\sigma^{(n)}\big) + c\epsilon_n \log d_n + \frac{o(\epsilon_n)}{n} \\ &\leq \frac{1}{n} E_F\big(\varrho^{\otimes n}\big) + c\epsilon_n \log d_n + \frac{o(\epsilon_n)}{n} \end{aligned}$$

for some constant c and $o(\epsilon_n)$ vanishing faster than ϵ_n in the limit of large n. Combining this with (3.8) one has

$$\frac{\log d_n}{n} \leq \frac{1}{n} E_F\big(\varrho^{\otimes n}\big) + c\epsilon_n \frac{\log d_n}{n} + \frac{o(\epsilon_n)}{n}.$$

Taking the limit on both sides, utilizing Eq. (3.7), and exploiting the fact that $K_D = \lim_n(\log d_n/n)$, we get finally the desired inequality that can be stated as follows (see [4, 5] for alternative proof):

Property 2. For any bipartite state ϱ

$$K_D(\varrho) \leq E_C(\varrho).$$

This immediately implies $K_D(\varrho) \leq E_F(\varrho)$ since E_F majorises E_C.

IV. CONCLUSIONS

We have proven that any d–dimensional private state, i.e., state that contains $\log d$ bits of perfectly secure key is distillable and we have provided the explicit LOCC operations of distillation protocol. This result has already been applied by other authors [8] in a proof of unconditional security with small distillable entanglement. We have also provided the analogous result for a multipartite version of d–dimensional private state which is a part of general scheme for distillation of multipartite key [14]. The results imply immediately that although from bound entanglement one can produce arbitrary secure bit of key (Eve's knowledge can be made arbitrarily small), the latter can never be perfectly secure (Eve's knowledge can not be made equal to zero). Finally exploiting the structure of eigenvectors of p-bits we have provided an elementary alternative proof of the fact that entanglement cost is an upper bound on the amount of distillable key of any quantum state.

Acknowledgments

R. A. thanks Maciej Demianowicz for fruitful discussions. This work was prepared under the (solicited) Polish Ministry of Scientific Research and Information Technology grant no. PBZ-MIN-008/P03/2003 and by EC grant RESQ, contract no. IST-2001-37559.

[1] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[2] D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996); N. Gisin and S. Wolf, *ibid.* **83**, 4200 (1999); D. Bruss *et al.*, *ibid.* **91**, 097901 (2003).

[3] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).

[4] K. Horodecki *et al.*, Phys. Rev. Lett. **94**, 160502 (2005).

[5] K. Horodecki *et al.*, quant-ph/0506189.

[6] C. H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996); N. Gisin, Phys. Lett. A **210**, 151 (1996).

[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).

[8] K. Horodecki *et al.*, Phys. Rev. Lett. **96**, 070501 (2006)

[9] P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A **34**, 6891 (2000).

[10] For review on entanglement measures see M. Horodecki, Quant. Inf. Comp. **1**, 3 (2001).

[11] Nonegativity of a_s $(s = 1, 2)$ stems from the fact that $\gamma^{(2)}$ is a state. To see that $\eta \leq \sqrt{a_1 a_2}$ one uses Cauchy-Schwarz inequality obtaining

$$\begin{aligned} \eta &= \left| \langle \tilde{e}_1| \otimes \langle \tilde{f}_1| U_0 \sqrt{\rho_{A'B'}} \sqrt{\rho_{A'B'}} U_1^\dagger |\tilde{e}_2\rangle \otimes |\tilde{f}_2\rangle \right| \\ &\leq \sqrt{\langle \tilde{e}_1| \otimes \langle \tilde{f}_1| U_0 \rho_{A'B'} U_0^\dagger |\tilde{e}_1\rangle \otimes |\tilde{f}_1\rangle} \\ &\quad \times \sqrt{\langle \tilde{e}_2| \otimes \langle \tilde{f}_2| U_1 \rho_{A'B'} U_1^\dagger |\tilde{e}_2\rangle \otimes |\tilde{f}_2\rangle} \\ &= \sqrt{a_1 a_2}. \end{aligned}$$

Since $\eta > 0$, both numbers a_s must be strictly positive.

[12] E. M. Rains, Phys. Rev. A **60**, 179 (1999); *ibid.* **63**, 019902(E) (2001).

[13] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3814 (1997).

[14] R. Augusiak and P. Horodecki, in preparation.

[15] E. N. Maneva and J. A. Smolin, in *AMS Contemporary Mathematics Series*, edited by S. J. Lomonaco and H. E. Brandt, vol. 305, (AMS, Providence, 2002), p. 203. See also quant-ph/0003099.

[16] P. Horodecki, R. Horodecki, and M. Horodecki, Acta Phys. Slov. **48**, 141 (1998).

[17] K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf, Phys. Rev. A **69**, 062304 (2004).

[18] M. Nielsen, Phys. Rev. A **61**, 064301 (2000).

[19] By LOCC protocol one means any LOCC operation that is trace-preserving.

[20] For a given state Ξ its von Neumann entropy reads $S_{\rm vN}(\Xi) = -{\rm Tr}\Xi \log \Xi$.

[21] See L. P. Hughston, R. Jozsa, and W. W. Wooters, Phys. Lett. A **183**, 14 (1993).